Spotwork.AI | Spotlab · Research & Insights

Collection
FIABILITÉ & GOUVERNANCE

SPOTLAB / ANALYSE P08

Gouvernance de l'IA : comment articuler AI Act, ISO 42001 et NIST AI RMF ?

Trois cadres complémentaires, mais non équivalents : une méthode en cinq décisions pour relier obligations, risques, contrôles et preuves.

Analyse / P08

Novembre 2026

Sources consultées au 2 novembre 2026

Use the best of AI.
Build your own intelligence.

ANALYSE P08

Sommaire

01	Trois enseignements pour les décideurs	3
02	AI Act, ISO 42001 et NIST : trois fonctions différentes	4
03	Le calendrier AI Act à ne pas simplifier abusivement	6
04	La méthode Spotwork.AI : relier l'obligation à la preuve	7
05	Cas professionnel : deux usages, deux niveaux de contrôle	9
06	Mesurer que la gouvernance fonctionne	10
07	Ce qu'un comité de direction devrait demander	10
08	Conclusion : un dispositif unique, des preuves distinctes	11
09	Questions fréquentes	11
10	Sources, méthode et limites	12

FICHE DE L'ANALYSE

ÉDITEUR
Spotwork.AI — Spotlab, Research & Insights

RÉFÉRENCE
P08

TYPE
Analyse documentaire

COLLECTION
Fiabilité & gouvernance

SOURCES CONSULTÉES
2 novembre 2026

PUBLICATIONS LIÉES
P07 · I0-02

EN BREF

Trois références dominent les discussions sur la gouvernance de l'intelligence artificielle. Elles ne sont ni interchangeables ni concurrentes : l'AI Act détermine ce qui est juridiquement exigé, ISO/IEC 42001 aide à organiser le management de l'IA, et le NIST AI RMF offre une méthode volontaire d'analyse et de traitement des risques. Pour les dirigeants, l'enjeu est de les traduire en un dispositif unique, proportionné aux usages, avec des décisions et des preuves réellement vérifiables.

> *Les cadres réglementaires, de management et de maîtrise des risques sont complémentaires. Leur articulation doit aboutir à des responsabilités et des contrôles concrets.*
>
> CE QU'IL FAUT RETENIR

01 Trois enseignements pour les décideurs

1

Commencer par les usages, pas par les normes.

Les obligations de l'AI Act varient selon le rôle de l'organisation, la finalité du système, sa qualification juridique et les échéances. Un assistant de rédaction et un système de sélection de candidats ne s'analysent pas de la même manière.

2

Une certification ne dispense pas de démontrer la conformité.

ISO/IEC 42001 porte sur un système de management. Elle ne certifie pas automatiquement chaque modèle ou usage, et ne remplace aucune obligation du droit européen.

3

La gouvernance se juge sur son fonctionnement réel.

Un registre, une politique et un comité ne prouvent pas à eux seuls qu'un système a été évalué, autorisé, surveillé et corrigé. Il faut relier les contrôles à des résultats et à des responsables.

TROIS QUESTIONS DISTINCTES

Qu'est-ce qui s'applique ? Comment gouverner durablement ? Quels risques mesurer et traiter ? **La valeur ne provient pas d'un « mapping » générique** prétendant faire correspondre chaque ligne de texte à une autre, mais d'un registre d'usages qualifiés, de responsables identifiés, de contrôles proportionnés, de décisions vérifiables et de preuves conservées dans le temps.

02 AI Act, ISO 42001 et NIST : trois fonctions différentes

Référence	Question à laquelle elle répond	Nature	Preuves à rechercher
AI Act	Quelles obligations s'appliquent à cet usage et à cette organisation ?	Règlement européen contraignant, selon disposition et calendrier	Qualification de l'usage et du rôle, obligations identifiées, conformité documentée
ISO/IEC 42001:2023	Comment organiser durablement la gouvernance de l'IA ?	Norme internationale de système de management ; adoption/certification volontaires	Politiques, responsabilités, périmètre, revues, amélioration, audits pertinents
NIST AI RMF 1.0	Comment comprendre, mesurer et traiter les risques ?	Cadre volontaire de gestion des risques, organisé en Govern, Map, Measure, Manage	Évaluations contextualisées, critères de mesure, décisions de traitement et suivi

ATTENTION À LA FAUSSE ÉQUIVALENCE

Les trois références ne possèdent pas les mêmes destinataires, périmètres ou niveaux d'exigence. Une organisation peut s'appuyer sur une seule activité de contrôle pour répondre à plusieurs besoins, mais elle doit démontrer séparément la satisfaction de chaque obligation applicable. Une procédure de revue humaine peut, par exemple, contribuer au management de l'IA, au suivi des risques et éventuellement à une obligation réglementaire ; toutefois la preuve exigée, la personne responsable et le moment de réalisation peuvent différer. Aucun certificat ISO/IEC 42001 ne constitue par lui-même une preuve générale de conformité à l'AI Act.

1. AI Act : établir d'abord le périmètre juridique

Le premier travail consiste à qualifier le système, l'usage, le rôle de l'organisation (notamment fournisseur ou déployeur), la catégorie de risque et la disposition applicable. Il faut aussi tenir compte des obligations transverses, notamment certaines pratiques interdites, la maîtrise de l'IA (AI literacy) et les règles de transparence lorsque les conditions sont réunies.

Par exemple, l'article 26 décrit les obligations des déployeurs de systèmes à haut risque, notamment le contrôle humain et la surveillance de l'usage. Mais ces dispositions ne doivent pas être présentées comme immédiatement exigibles dans tous les cas d'usage en 2026 : leur applicabilité dépend du système et du calendrier [3].

02 / TROIS FONCTIONS DIFFÉRENTES — SUITE

2. ISO/IEC 42001 : installer une organisation qui dure

ISO/IEC 42001:2023 définit des exigences pour établir, mettre en œuvre, maintenir et améliorer un système de management de l'IA. Sa portée concerne des organisations qui développent, fournissent ou utilisent des produits et services intégrant de l'IA. Elle est utile pour relier la stratégie, les responsabilités, l'évaluation, le suivi et l'amélioration continue [4].

La certification, lorsqu'elle est choisie, est réalisée par un organisme de certification indépendant, et non par l'ISO elle-même. Elle porte sur le système de management et son périmètre certifié, pas sur une garantie universelle de sûreté de chaque résultat de modèle [5].

La présente publication utilise la description publique de l'ISO/IEC 42001. Elle ne reproduit pas la norme intégrale, soumise à licence, et ne prétend pas produire un tableau exhaustif de correspondance des clauses.

3. NIST AI RMF : donner une méthode aux équipes risques et métiers

Le NIST AI RMF 1.0 organise ses recommandations autour de quatre fonctions complémentaires : Govern (gouverner), Map (contextualiser et identifier), Measure (mesurer) et Manage (traiter et suivre). Son Playbook suggère des actions adaptables : il ne doit pas être lu comme une liste obligatoire à appliquer intégralement à chaque système [6][7].

GOVERN	MAP	MEASURE	MANAGE
Gouverner	Contextualiser et identifier	Mesurer	Traiter et suivre

Le cadre permet notamment de structurer un test de fiabilité : quelles tâches ont été évaluées, sur quels exemples, avec quels critères, dans quelles conditions et avec quels résultats ? Les erreurs critiques et les actions correctives doivent rester visibles, y compris lorsque la moyenne globale paraît favorable (voir « Comment évaluer la fiabilité d·une IA générative en entreprise ? Un protocole en sept étapes »).

03 Le calendrier AI Act à ne pas simplifier abusivement

Au 2 novembre 2026, le règlement a déjà connu une modification importante : le règlement (UE) 2026/1744, entré en vigueur le 27 juillet 2026, a repoussé l'application des principales exigences de haut risque de l'annexe III au 2 décembre 2027, et de celles liées aux produits réglementés de l'annexe I au 2 août 2028. D'autres dispositions s'appliquent déjà. La date ne doit donc jamais être déduite de la seule mention « AI Act » [1][2][3]. Le règlement modificatif a été adopté le 8 juillet 2026 et publié au Journal officiel le 24 juillet 2026.

Date	Régime ou jalon principal	Implication pratique
2 février 2025	Pratiques interdites et mesures de maîtrise de l'IA	Contrôler les usages interdits et adapter les mesures d'AI literacy
2 août 2025	Obligations GPAI et gouvernance (avec transitions)	Identifier les obligations selon le rôle de l'organisation
2 août 2026	Application de la plupart des autres dispositions, notamment certaines obligations de transparence	Identifier les usages soumis à information ou transparence
2 décembre 2026	Interdictions ciblées ajoutées en 2026 ; fin du délai de marquage (art. 50 §2) pour les fournisseurs de systèmes générant des contenus synthétiques mis sur le marché avant le 2 août 2026 (art. 111 §4)	Ne pas étendre ce report à tous les usages
2 décembre 2027	Principales exigences des systèmes à haut risque de l'annexe III	Préparer les dossiers des usages concernés
2 août 2028	Principales exigences des systèmes à haut risque liés aux produits de l'annexe I	Préparer les cas visés par ce cadre particulier

IMPORTANT

La date seule ne prouve jamais qu'un usage est classé « haut risque ». La qualification doit s'appuyer sur le texte applicable, sa finalité, l'annexe concernée, d'éventuelles exceptions et le rôle effectivement exercé. Les obligations relatives aux données personnelles et à la sécurité peuvent s'appliquer par ailleurs, indépendamment de ces jalons. Le détail du calendrier et de la qualification est traité dans notre analyse « AI Act 2026 : quelles obligations s·appliquent réellement aux entreprises ? ».

04 La méthode Spotwork.AI : relier l'obligation à la preuve

À partir des trois référentiels, Spotwork.AI propose une chaîne de pilotage en cinq décisions. Il s'agit d'une proposition méthodologique, pas d'un mécanisme officiel de certification ou de correspondance juridique. Elle doit pouvoir s'appliquer aussi bien à un outil de productivité qu'à un système plus sensible, à condition d'adapter les contrôles et les seuils.

Décision	Question de direction	Livrable de contrôle	Critère de passage
1. Qualifier	Quels usages, quel rôle et quelles règles applicables ?	Registre des systèmes, classification et justification	Classification argumentée, réserves et échéances identifiées
2. Attribuer	Qui décide, qui opère, qui contrôle ?	Responsable identifié et droits d'approbation	Propriétaire, évaluateur et décideur identifiés
3. Évaluer	Quels risques et critères d'acceptation par usage ?	Protocole de test, résultats, limites et niveau de risque	Erreurs bloquantes évaluées ; acceptabilité établie
4. Autoriser	Peut-on déployer, sous quelles conditions ?	Décision tracée : accepter, conditionner, corriger ou refuser	Traçabilité de la décision et de ses conditions
5. Surveiller	Que fait-on si le contexte ou le modèle change ?	Suivi des incidents, versions, réévaluations et remédiations	Révision déclenchée quand l'usage ou le risque évolue

LE POINT DE JONCTION EST UNE PREUVE EXPLOITABLE

Une « politique de contrôle humain » n'est pas équivalente à la preuve qu'une personne habilitée a effectivement examiné une décision sensible. De même, un score moyen satisfaisant ne suffit pas à établir la maîtrise d'un risque critique.

La décision « Qualifier » s'appuie sur la grille de qualification réglementaire détaillée dans notre analyse P07 — AI Act 2026 (recenser, qualifier, dater).

04 / DU TEXTE AU DISPOSITIF DE GOUVERNANCE

Trois couches distinctes, reliées entre elles

A

Obligations et politiques

Catalogue des usages, périmètre juridique, droits et obligations applicables, standards internes, niveau de tolérance au risque et responsabilités.

B

Contrôles opérationnels

Tests documentaires, règles de revue, conditions d'autorisation, accès aux données, journalisation, validation humaine pertinente et maîtrise des changements.

C

Preuves et décisions

Version du système, date et protocole de test, résultat, écart, responsable de la décision, remédiation, événement de revalidation et historique de changement.

La preuve est le lien entre ces couches. Un contrôle planifié mais jamais réalisé est un dispositif incomplet ; un test réussi sur une ancienne version peut perdre sa valeur après un changement du modèle, du corpus ou des outils.

Conditions d'intégration dans un cadre d'entreprise

Un dispositif opérationnel doit éviter deux excès. Le premier serait de multiplier les formalités de conformité pour de simples usages de productivité ; le second serait de considérer qu'un système n'a pas besoin de gouvernance tant qu'il n'est pas classé à haut risque au sens de l'AI Act.

La bonne approche : réutiliser les mécanismes de risques, de sécurité, de contrôle interne et de gouvernance déjà en place, puis ajouter les éléments IA spécifiques nécessaires. Un inventaire unique et une chaîne de preuves partagée peuvent réduire les redondances sans effacer les responsabilités propres à chaque obligation.

Dans le cadre de cette étude, Spotwork.AI illustre une logique de gestion et de production de preuves. Cela n'implique ni que le produit certifie un système de management, ni qu'il prononce une décision de conformité réglementaire.

05 Cas professionnel : deux usages, deux niveaux de contrôle

Prenons une entreprise qui déploie deux applications différentes.

CAS A

Assistant de synthèse documentaire interne

Il résume des comptes rendus et propose des premières versions de notes, qu'un professionnel vérifie avant usage. Sa qualification juridique ne peut pas être présumée à partir du seul mot « IA ». Le dispositif doit néanmoins traiter confidentialité, sources, droits d'accès, qualité des livrables et traçabilité, avec des contrôles proportionnés.

Contrôles illustratifs : corpus autorisé et horodaté ; test de fidélité et de couverture ; refus des accès hors périmètre ; validation par un responsable pour les livrables sensibles ; suivi des erreurs ; re-test après modification du modèle ou de la base documentaire.

Décision possible : déploiement limité si les cas critiques sont satisfaits ; correction si des sources internes non autorisées sont visibles ; arrêt si le cloisonnement des données ne tient pas.

CAS B

Système de présélection de candidatures

Un outil qui analyse et classe des candidatures pour aider au recrutement peut relever des cas à haut risque visés par l'annexe III, selon sa finalité et les règles de classification applicables. La qualification doit être établie et les obligations correspondantes préparées dans le calendrier réglementaire. Un dispositif de gouvernance sérieusement conçu doit également documenter les risques de discrimination, les données utilisées, la supervision humaine et les mécanismes de contestation.

Contrôles illustratifs : vérification des données, biais et impacts possibles ; protocole d'évaluation ; compétences des personnes chargées du contrôle humain ; trace des décisions ; gestion des contestations ; supervision des changements.

Décision possible : suspendre la mise en service si la gouvernance ne permet pas de vérifier une discrimination majeure ; demander des corrections et de nouveaux tests avant tout élargissement du périmètre.

> *Standardiser la méthode de gouvernance, mais adapter les contrôles à chaque usage. Une politique uniforme sur les « modèles d'IA » ne suffit ni à piloter les risques ni à démontrer les obligations pertinentes.*

05 / LA LEÇON

06 Mesurer que la gouvernance fonctionne

Les indicateurs suivants sont des suggestions méthodologiques, à adapter à chaque activité et non des seuils officiels AI Act, ISO ou NIST :

Couverture	Part des usages significatifs identifiés et qualifiés, avec responsable et classification à jour.
Preuve	Part des contrôles essentiels disposant d'une preuve datée, associée à la version correcte.
Décision	Part des mises en service et changements importants ayant reçu une approbation explicite.
Qualité	Incidents critiques, erreurs non détectées, taux de cas satisfaisant les critères prédéfinis.
Réactivité	Délai d'identification et de traitement des écarts ; réévaluations réalisées lorsque les conditions changent.

La gouvernance échoue souvent lorsque des indicateurs de complétude documentaire remplacent le jugement sur le fonctionnement effectif des contrôles. Un registre entièrement rempli ne constitue pas une preuve de résultats maîtrisés.

07 Ce qu'un comité de direction devrait demander

Pour chacun des usages significatifs, cinq questions permettent de distinguer une politique de principe d'une gouvernance opérationnelle :

- Pourquoi ce système est-il utilisé ?
- Qui en assume la responsabilité ?
- Qu'a-t-on réellement testé ?
- Quelle décision autorise son usage ?
- Que se passe-t-il lorsqu'il change ou échoue ?

Ces questions peuvent être posées sans attendre une certification ni l'application de toutes les dispositions à haut risque. Elles permettent de construire une maîtrise progressive, adaptée à l'activité et aux moyens disponibles.

08 Conclusion : un dispositif unique, des preuves distinctes

L'AI Act fixe des obligations, ISO/IEC 42001 donne un cadre de management et le NIST AI RMF propose une lecture opérationnelle des risques. **Leur complémentarité devient utile lorsqu'une organisation relie, pour chaque système, l'usage, les règles, les personnes responsables, les tests, les décisions et le suivi.**

Pour Spotwork.AI, cette logique s'inscrit dans une ambition plus large : mobiliser les meilleures capacités de l'IA tout en préservant des méthodes, des connaissances et des contrôles propres à chaque organisation. Ce cadre éclaire cette démarche ; il ne constitue pas une attestation de conformité ni un avis juridique.

09 Questions fréquentes

Une certification ISO/IEC 42001 suffit-elle pour respecter l'AI Act ?

Non. Elle porte sur un système de management dans un périmètre donné. Les obligations réglementaires doivent être identifiées et démontrées séparément.

Le NIST AI RMF est-il obligatoire pour une entreprise française ?

Non en tant que tel : c'est un cadre volontaire. Il peut être utilisé pour organiser des évaluations et des contrôles dans un dispositif soumis par ailleurs à des obligations juridiques.

Faut-il attendre décembre 2027 pour mettre en place une gouvernance ?

Non. Plusieurs dispositions de l'AI Act s'appliquent déjà et des risques opérationnels existent indépendamment du calendrier. Les exigences futures doivent être anticipées selon les usages.

10 Sources, méthode et limites

Analyse documentaire des versions publiques officielles disponibles au 2 novembre 2026 : AI Act consolidé, règlement modificatif 2026/1744, calendrier Commission, ISO/IEC 42001, NIST AI RMF et NIST Playbook. La norme ISO intégrale étant soumise à licence, cette publication ne reproduit pas ses exigences internes ni ne revendique un mapping exhaustif clause par clause. Les exemples sont illustratifs. Une revue juridique spécialisée reste nécessaire pour les qualifications de cas particuliers.

Cette note confronte des références de nature hétérogène : un texte réglementaire consolidé, une norme de management accessible principalement sous licence, et un cadre de gestion des risques volontaire publié librement. Elle n'établit pas de relation normative clause à clause, ne valide aucune certification et ne constitue pas un avis juridique.

La structure du NIST AI RMF 1.0 reste une référence officielle, mais le NIST indique qu'une révision est en cours. La publication emploie ses quatre fonctions dans la version 1.0.

[1] Règlement (UE) 2024/1689 (AI Act), version consolidée.
eur-lex.europa.eu/eli/reg/2024/1689

[2] Règlement (UE) 2026/1744 du 8 juillet 2026, entré en vigueur le 27 juillet 2026.
eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32026R1744

[3] Commission européenne, AI Act Service Desk — calendrier de mise en œuvre ; article 26.
ai-act-service-desk.ec.europa.eu/en/ai-act/eu-ai-act-implementation-timeline · ai-act-service-desk.ec.europa.eu/fr/ai-act/article-26

[4] IEC, ISO/IEC 42001:2023 — présentation officielle.
webstore.iec.ch/en/publication/90574

[5] ISO, ISO/IEC 42001 explained ; ISO, Help — certification bodies.
iso.org/fr/home/insights-news/resources/iso-42001-explained-what-it-is.html

[6] NIST, AI Risk Management Framework (AI RMF 1.0).
nist.gov/itl/ai-risk-management-framework

[7] NIST, AI RMF Playbook.
airc.nist.gov/airmf-resources/playbook/

[8] NIST, Generative AI Profile (NIST AI 600-1).
nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence

Spotwork.AI

L'IA professionnelle de confiance

Mieux travailler aujourd'hui,
construire votre intelligence de demain.

SPOTLAB · RESEARCH & INSIGHTS · ANALYSE P08

Gouvernance de l'IA : comment articuler AI Act, ISO 42001 et NIST AI RMF ?

Une méthode en cinq décisions pour relier obligations, risques, contrôles et preuves

© 2026 SPOTWORK.AI